Claims

1. A conditional access system comprising a first transmitter for transmitting a scrambled broadcast stream and a second transmitter for transmitting a plurality of control messages separate from the broadcast stream, said control messages including information for descrambling the broadcast stream.

2. A conditional access system according to claim 1, wherein said control messages are alone sufficient to permit the broadcast stream to be descrambled.

3. A conditional access system according to claim 1, wherein said information for descrambling the broadcast stream is incorporated into each of said control messages without being encrypted.

4. A conditional access system according to claim 1, wherein said information for descrambling the broadcast stream is encrypted prior to being incorporated into each of said control messages.

5. A conditional access system according to claim 1, further comprising a scrambler and a key generator for generating a stream of encryption keys, the scrambler being operable to encrypt a broadcast stream with the encryption key stream, the system further being operable to send the encryption key stream to a decoder for decoding the encrypted broadcast stream, said encrypted key stream comprising the information for descrambling the broadcast stream.

6. A conditional access system according to claim 1, wherein the second transmitter is arranged to transmit the descrambling information to a receiver using a point-to-point protocol.

7. A conditional access system according to claim 1, wherein the second transmitter is arranged to transmit the descrambling information over a secure connection.

8. A conditional access system according to claim 7, wherein the secure connection comprises a virtual private network (VPN).

9. A conditional access system according to claim 1, wherein the control message comprises an entitlement control message (ECM).

10. A conditional access system comprising a first receiver for receiving a scrambled broadcast stream and a second receiver for receiving a plurality of control messages separate from the broadcast stream, the control messages including information for descrambling the broadcast stream.

11. A conditional access system according to claim 10, wherein the control messages are sent to the second receiver using a point-to-point protocol.

12. A conditional access system according to claim 10, wherein the control messages are sent to the second receiver over a secure connection.

13. A conditional access system according to claim 12, wherein the secure connection comprises a virtual private network (VPN).

14. A conditional access system according to claim 10, wherein the control messages comprise entitlement control messages (ECMs).

15. A conditional access system according to claim 10, further comprising a decoder for descrambling the broadcast stream in accordance with the descrambling information.

16. A conditional access system according to claim 10, wherein said information for descrambling the broadcast stream is incorporated into said control messages without being encrypted, whereby the decoder does not require a smart card for decryption.

17. A conditional access system according to claim 10, wherein said second receiver comprises a mobile telephone.

18. A decoder for use in a conditional access system for decrypting encrypted broadcast content, comprising:

a first input module for receiving said encrypted broadcast content from a first communications channel;

a second input module for receiving a plurality of control messages from a second communications channel, said control messages containing descrambling information for decrypting said broadcast content.

19. A decoder according to claim 18, further comprising a processor module for extracting said descrambling information from said control messages.

20. A decoder according to claim 19, further comprising a descrambler for receiving said encrypted broadcast content and decrypting said content using said descrambling information.

21. A method for use in a conditional access system, in which a scrambled broadcast stream is transmitted to a decoder, said decoder being operable to receive a plurality of control messages including information for descrambling the broadcast stream, the method comprising sending said control messages to said decoder separately from said broadcast stream.

22. A method according to claim 21, comprising incorporating said descrambling information into the control messages without encrypting it.

23. A method according to claim 22, comprising encrypting the control messages prior to sending them to the decoder.

24. A method according to claim 21, comprising sending the control message over a secure channel.

25. A method according to claim 24, wherein the secure channel comprises a virtual private network.

26. A method for use in a conditional access system, in which a scrambled broadcast stream is transmitted to a first decoder and a second decoder, said first and second decoders being operable to receive a plurality of control messages including information for descrambling the broadcast stream, the method comprising receiving a request to transmit a plurality of control messages to said second decoder separately from the broadcast stream.

27. A method according to claim 26, wherein said control messages are alone sufficient to descramble said broadcast stream.

28. A method according to claim 26, further comprising denying a service to the first decoder while the plurality of control messages is being sent to the second decoder.

29. A conditional access system, comprising:

a first communications channel for carrying a broadcast stream, said stream being scrambled with a stream of control words;

a second communications channel separate from the first channel for carrying a stream of entitlement control messages, said entitlement control messages incorporating information relating to the stream of control words for descrambling the broadcast stream.

30. A conditional access system according to claim 29, wherein said entitlement control messages alone contain all of the information required to descramble the broadcast stream.